

# CRS Report for Congress

Received through the CRS Web

## **Homeland Security Advisory System: Possible Issues for Congressional Oversight**

**August 6, 2003**

Shawn Reese  
Analyst in American National Government  
Government and Finance Division

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>06 AUG 2003</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2003 to 00-00-2003</b>	
4. TITLE AND SUBTITLE <b>Homeland Security Advisory System: Possible Issues for Congressional Oversight</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Congressional Research Service, The Library of Congress, 101 Independence Ave SE, Washington, DC, 20540-7500</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>17</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

# Homeland Security Advisory System: Possible Issues for Congressional Oversight

## Summary

The Homeland Security Advisory System (HSAS), established on Mar. 12, 2002, is a color coded terrorist threat warning system administered by the Department of Homeland Security (DHS). The system, which federal departments and agencies are required to implement and use, provides recommended protective measures for federal departments and agencies to prevent, prepare for, mitigate against, and respond to, terrorist attacks.

DHS disseminates HSAS terrorist threat warnings to federal departments, state and local agencies, the public, and private sector entities. This dissemination of warnings is conducted through multiple communication systems and public announcements.

HSAS has five threat levels: low; guarded; elevated; high; or severe. From March, 2002, to July, 2003, the HSAS threat level has been no lower than elevated, and has been raised to high four times. The first time it was raised to high was on September 10, 2002 due to the fear of terrorist attacks on the anniversary of the terrorist attacks of Sept. 11, 2001, and the most recent time it was raised to high was May 20, 2003 due to terrorist bombings in Saudi Arabia and Morocco.

While the need for terrorist threat warnings seems to be widely acknowledged, there are numerous issues associated with HSAS and its effects on states, localities, the public, and the private sector. These issues include the following:

- vagueness of warnings;
- lack of specific protective measures for state and local governments, the public, and the private sector;
- dissemination of warnings to states, localities, the public, and the private sector;
- coordination of HSAS with other federal warning systems; and,
- cost of threat level changes.

This report will be updated as congressional or executive actions warrant.

## Contents

Threat Conditions .....	1
Issues .....	4
Vagueness of Warnings .....	4
Lack of Specific Protective Measures for State and Local Governments, the Public, and the Private Sector .....	6
Communication of Terrorist Threats to State and Local Governments, the Public, and the Private Sector .....	8
Coordination of HSAS with Other Warning Systems .....	9
Cost of Threat Level Changes .....	12

## List of Tables

Table 1. HSAS Threat Levels .....	2
-----------------------------------	---

## List of Figures

Figure 1. Homeland Security Threat Level Changes. ....	15
--	----

# Homeland Security Advisory System: Possible Issues for Congressional Oversight

On March 12, 2002, Governor Tom Ridge—then Director of the White House Office of Homeland Security (OHS), and now Secretary of the Department of Homeland Security (DHS)—announced the establishment of the Homeland Security Advisory System (HSAS). The HSAS is designed to measure and evaluate terrorist threats and communicate these threats to federal, state, and local governments, the public, and the private sector in a timely manner. Although HSAS is a nationwide system, it can also be used at a smaller scale to warn of threats against a state, city, critical infrastructure, or industry.<sup>1</sup> Since inception to July 2003, the HSAS has been raised from “Elevated” to “High” four times—see Figure 1 on page 15 of this report.

The HSAS was developed by OHS using information collected from state and local first responders, business leaders, and the public. Following the March 12 announcement, the general public and the private sector were asked to provide comments on the system, with a deadline for comments on April 26, 2002.<sup>2</sup>

Within DHS, the Undersecretary for Information Assurance and Infrastructure Protection—as head of the Information Assurance and Infrastructure Protection directorate (IAIP)—is responsible for administering the HSAS. Specifically, IAIP is responsible for providing, in coordination with other agencies of the federal government, specific warning information and advice about appropriate protective measures and countermeasures to state and local government agencies and authorities, the private sector, other entities, and the public.<sup>3</sup>

## Threat Conditions

The advisory system is based on five threat levels: low, guarded, elevated, high, and severe. Each level, with its corresponding identification color, indicates protective measures mandatory for federal departments and agencies.<sup>4</sup>

---

<sup>1</sup> Office of the White House Press Secretary, “Remarks by Governor Ridge Announcing Homeland Security Advisory System,” press release, (Washington: March 12, 2002). Available at [<http://www.whitehouse.gov/news/releases/2002/03/20020312-14.html>], visited March 15, 2003.

<sup>2</sup> Ibid.

<sup>3</sup> P.L. 107-296, Title II, subtitle A, sec. 201(d)(7).

<sup>4</sup> U.S. President (Bush), “Homeland Security Advisory System,” Homeland Security Presidential Directive 3, March 11, 2002. Available at: [<http://www.whitehouse.gov/news/releases/2002/03/20020312-5.html>], visited Jun. 3, 2003.

**Table 1. HSAS Threat Levels**

<b>Threat Level</b>	<b>Risk of Terrorist Attack</b>	<b>Protective Measures</b>
GREEN Low	Low	<ul style="list-style-type: none"> <li>- Refine preplanned protective measures</li> <li>- Ensure personnel trained on HSAS and preplanned protective measures</li> <li>- Institutionalize a process for assuring all facilities are assessed for vulnerabilities and measures are taken to mitigate these vulnerabilities</li> </ul>
BLUE Guarded	General	<ul style="list-style-type: none"> <li>- Check emergency response communications</li> <li>- Review and update emergency response procedures</li> <li>- Provide information to public that would strengthen its ability to react to an attack</li> </ul>
YELLOW Elevated	Significant	<ul style="list-style-type: none"> <li>- Increase surveillance of critical locations</li> <li>- Coordinate emergency plans with other federal, state, and local facilities</li> <li>- Assess the threat and refine protective measures as necessary</li> <li>- Implement emergency response plans</li> </ul>
ORANGE High	High	<ul style="list-style-type: none"> <li>- Coordinate security efforts with federal, state, and local law enforcement agencies</li> <li>- Take additional protective measures at public events, changing venues, or consider cancelling if necessary</li> <li>- Prepare to execute contingency operations</li> <li>- Restrict facility access to essential personnel</li> </ul>
RED Severe	Severe	<ul style="list-style-type: none"> <li>- Increase or redirect personnel to address critical emergency needs</li> <li>- Assign emergency response personnel and mobilize specially trained teams</li> <li>- Monitor, and redirect transportation systems</li> <li>- Close public and government facilities</li> </ul>

Source: U.S. President (Bush), "Homeland Security Advisory System," Homeland Security Presidential Directive 3, March 11, 2002. Available at [<http://www.whitehouse.gov/news/releases/2002/03/2002312-5.html>], visited Jun. 3, 2002.

DHS receives threat information from the Federal Bureau of Investigation, the Central Intelligence Agency, the National Security Agency, the Drug Enforcement Agency, the Department of Defense (DOD), and other agencies. DHS uses this information to determine what terrorist threat level to set.<sup>5</sup>

<sup>5</sup> U.S. Department of Homeland Security, "Threats & Protection: Synthesizing and Disseminating Information," [[http://www.dhs.gov/dhspublic/theme\\_home6.jsp](http://www.dhs.gov/dhspublic/theme_home6.jsp)], visited Jun. 3, 2003.

Assigning a threat condition involves a variety of considerations, among which are the following:

- To what degree is the threat information credible?
- To what degree is the threat information corroborated?
- To what degree is the threat specific and imminent?
- How grave are the potential consequences of the threat?<sup>6</sup>

The DHS Secretary decides to raise or lower the threat level in consultation with the Homeland Security Council.<sup>7</sup> When the decision to change the threat level is made, DHS sends an electronic notification to state homeland security centers, and federal, state and local agencies via the National Law Enforcement Telecommunications System (NLETS).<sup>8</sup> If circumstances and time permit, however, the DHS Secretary or his representative makes an advance conference call to alert Governors, state homeland security advisors, and mayors of selected cities that the terrorism threat level has been changed and that electronic notification is about to be sent.

#### **Homeland Security Council Membership**

Secretary of Homeland Security  
 Secretary of the Treasury  
 Secretary of Defense  
 Attorney General  
 Secretary of Health and Human Services  
 Secretary of Transportation  
 Director of Office Management and Budget  
 Director of Central Intelligence  
 Director of Federal Bureau of Investigation  
 Director of Federal Emergency Management Agency  
 Chief of Staff to the President  
 Chief of Staff to the Vice President  
**Source:** Executive Office of the President, "Fact Sheet: Homeland Security Council," press release, Oct. 29, 2001.

Following the first conference call and electronic notification via NLETS, DHS makes a second conference call to as many state and local law enforcement associations as can be reached. Following the second conference call, DHS initiates

---

<sup>6</sup> U.S. President (Bush), "Homeland Security Advisory System," Homeland Security Presidential Directive 3, March 11, 2002.  
 Available at [<http://www.whitehouse.gov/news/releases/2002/03/20020312-5.html>], visited June 3, 2003.

<sup>7</sup> U.S. Department of Homeland Security, "Threats & Protection: Advisory System," <http://www.dhs.gov/dhspublic/display?theme=29>, visited May 12, 2003.

<sup>8</sup> U.S. Congress, Senate Governmental Affairs Committee, *State and Local Homeland Security Challenges*, unprinted hearing of 108<sup>th</sup> Cong., 1<sup>st</sup> sess., May 1, 2003.

a secure call using the Business Roundtable's Critical Emergency Operations Communications Link (CEO COM LINK) to notify chief executive officers of the nation's top businesses and industries.<sup>9</sup> They are asked to dial into a secure conference call, and after each CEO goes through a multi-step authentication process to ensure security, DHS or other federal officials brief them on developments and threats.<sup>10</sup>

Following the conference call via CEO COM LINK, DHS makes a public announcement through a press conference. Finally, critical infrastructure associations and other business groups are notified.<sup>11</sup>

## Issues

Since the creation of the HSAS, a number of issues has arisen, among which are: the vagueness of warnings disseminated by the system; the system's lack of protective measures recommended for state and local governments and the public; the perceived inadequacy of disseminating threats to state and local governments, the public, and the private sector; and how best to coordinate HSAS with other existing warning issues. These issues and pertinent oversight options available to Congress are discussed below.

### Vagueness of Warnings

The HSAS threat level has been raised four times from "Yellow" to "Orange" since its activation on March 12, 2002. With each change, the Attorney General or DHS Secretary cited intelligence information but offered no specifics. No federal facilities, regions, states, localities, or private sector entities were identified as being at special risk. Moreover, DHS has never explained the sources and quality of intelligence upon which the threat levels were based.<sup>12</sup>

**Analysis and Options.** Some observers have asserted that when federal government officials announce a new warning about terrorist attacks, the threats are

---

<sup>9</sup> CEO COM LINK is a secure telecommunications network that is activated during national crises and threats. Due to the sensitive nature of CEO COM LINK, a list of businesses and industries that participate in the system is not publicly available.

<sup>10</sup> Business Roundtable, "Questions and Answers on CEO COM LINK," [<http://www.brtable.org/document.cfm/760>], visited May 12, 2003.

<sup>11</sup> U.S. Congress, Senate Governmental Affairs Committee, *State and Local Homeland Security Challenges*, May 1, 2003.

<sup>12</sup> Eunice Moscoso, "Government Hikes Terror Alert Status to 'High'," *Cox News Service*, Sept. 10, 2002, sec. Washington, General News. "Threats and Responses," *The New York Times*, Sept. 11, 2002, p. A12. U.S. Department of Homeland Security, Office of Press Secretary, "Statement by Homeland Security Secretary Tom Ridge on Raising Threat Level," press release, May 20, 2003, available at: [<http://www.dhs.gov/dhspublic/display?content=741>], visited Jun. 4, 2003. Allyson Price, U.S. Department of Homeland Security, Congressional Liaison, telephone conversation with author, Jun. 20, 2003.



too vague.<sup>13</sup> The vagueness that characterized the four increases in the threat condition in the past two years has raised concerns that the public may begin to question the authenticity of the HSAS threat level. Secretary Ridge told reporters on June 6, 2003, that DHS is worried about the credibility of the system. He said that the system needs to be further refined.<sup>14</sup>

Questions about the credibility of the threat, say other observers, might cause the public to wonder how to act or whether to take any special action at all. Some observers maintain that, without specific terrorist threat information, there is no basis for formulating a clear, easily understood public announcement of what appropriate protective measures to take.<sup>15</sup> Others assert that the continued lack of specific information arguably can lead to complacency.<sup>16</sup>

DHS officials cite the lack of specificity in intelligence as the reason for a lack of detailed information when the threat level is changed. Secretary Ridge has been quoted saying that the intelligence gathered so far has been generic; but he maintained that DHS, and the federal intelligence community that provides information about terrorist threats, will improve.<sup>17</sup>

*Option 1: Status quo.* Congress may view the evolution of the process, and decisions relating to it are best left to the Department. The lack of specificity may be due to the need to protect intelligence sources or a desire by DHS to issue warnings when threat information is generic, but nonetheless credible. Maintaining the status quo places the burden of responding to complaints about the vagueness of HSAS warnings and the critiques of DHS's perceived inability to give adequate terrorist attack warnings on the Department.

*Option 2: Provide general warnings.* Due to the reported misunderstanding of HSAS threat levels, and the system's lack of recommended protective measures for state and local agencies, the public, and private sector entities, Congress could consider directing DHS to issue general warnings concerning the threat of terrorist attacks *without* using the HSAS to notify state and local governments, the public, and the private sector. General warnings via public statements, in coordination with HSAS warnings to the federal government, would ensure that notices of terrorist threats are issued to state and local governments, the public, and the private sector. This approach would address the concerns of some who have asserted that the HSAS causes misunderstanding at the state and local level, but it would not address the

---

<sup>13</sup> Dan Barry, and Al Baker, "Security Tighter in New York After Vague Terrorist Threat," [http://www.nytimes.com/2002], visited May 22, 2002. Philip Shenon, "Suicide Attacks Certain in U.S., Mueller Warns," [http://www.nytimes.com/2002], visited May 21, 2002.

<sup>14</sup> John Mintz, "Ridge Seeking Fewer Changes in Terror Alerts," *The Washington Post*, June 6, 2003, sec. p. A11.

<sup>15</sup> Ross Kerber, "The Palette of Warning Terror-Alert System Called Inadequate," *The Boston Globe*, May 31, 2003, sec. Business, p. C1.

<sup>16</sup> David A. Fahrenthold, "This Time, Orange Alert Seems Less So," *The Washington Post*, May 22, 2003, p. B2.

<sup>17</sup> Ibid.

issue raised by those who say DHS does not give enough specificity in its terrorist attack warnings.

*Option 3: Increase specificity of warnings.* Were Congress to decide that the terrorist warnings issued by DHS are too vague and cause complacency in state and local agencies, the public, and the private sector, it might instruct DHS to use the HSAS to provide specific warnings to targeted federal facilities, regions, states, localities, and private sector industries to the extent that is possible. DHS has said that its goal is to have the capability to issue high alerts to designated cities, geographical regions, industry, or critical infrastructure.<sup>18</sup> This approach arguably would address the concerns about the perceived vagueness of HSAS warnings.

## **Lack of Specific Protective Measures for State and Local Governments, the Public, and the Private Sector**

The HSAS provides a set of protective measures for each threat condition, but these protective measures are identified only for federal agencies. DHS does not recommend protective measures for states, localities, the public, or the private sector.

**Analysis and Options.** HSAS silence with regard to protective measures for the public, the private sector, and state and local governments has drawn the attention of some interested observers. Early on, William B. Berger, President of the International Association of Chiefs of Police, testified before the Senate Governmental Affairs Committee that the lack of defined response protocols for state and local governments was an area of concern among local law enforcement agencies.<sup>19</sup>

Citing what some contend is a lack of DHS guidance on protective measures, non-federal entities are beginning to fill the perceived void. For example, the American Red Cross recommends protective measures for individuals, families, neighborhoods, schools and businesses at each of the HSAS threat levels.<sup>20</sup> Further, the State of Maryland has adopted the American Red Cross protective measures.<sup>21</sup>

---

<sup>18</sup> Ibid.

<sup>19</sup> U.S. Congress, Senate Governmental Affairs Committee, *Communities and Homeland Security*, unprinted hearing of the 107<sup>th</sup> Cong., 2<sup>nd</sup> sess., Dec. 11, 2001.

<sup>20</sup> American Red Cross, "American Red Cross Homeland Security Advisory System Recommendations for Individuals, Families, Neighborhoods, Schools, and Businesses," [<http://www.redcross.org/services/disaster/beprepared/hsas.html>], visited June 3, 2003.

<sup>21</sup> Maryland Emergency Management Agency, "Overview of the Maryland Threat Alert System and Guidance for Citizens, Schools, and Businesses," [[http://www.memo.domestic-preparedness.net/documents/mtas\\_public.pdf](http://www.memo.domestic-preparedness.net/documents/mtas_public.pdf)], visited June 10, 2003.

Without federal guidance, some cities have adopted the following types of protective measures when the HSAS threat condition is raised to “Orange”:

- Surveillance cameras are activated.
- Law enforcement officers are not granted time off.
- Port security patrols are increased.
- Law enforcement officers are required to carry biological/chemical protective masks.
- First responders are placed on alert.
- Mass transit authorities broadcast warnings and instructions.
- Mass transit law enforcement officers increase patrols.
- Law enforcement agencies make security checks in sensitive areas, such as bridges, shopping centers, religious establishments, and courthouses.<sup>22</sup>

*Option 1: Status quo.* The HSAS was designed for federal government use and Congress may deem the system adequate for the federal government. This approach can encourage states and localities to conduct threat and vulnerability assessments that would then assist in the development of specific protective measures geared to each state and locality’s homeland security needs. On the other hand, this approach might cause confusion among states and localities in their attempts to prepare for terrorist attacks without federal guidance on protective measures from the federal government.

*Option 2: Federal guidelines for state and local protective measures.* If Congress decided that there were a need for more guidance for states, localities, the public, and the private sector, it could either encourage DHS to establish HSAS protective measure guidance for states, localities, the public, and the private sector, or it could enact legislation mandating these activities. These protective measures could match the federal government preparedness and response activities identified in the HSAS. This approach could provide federal government guidance on how to be prepared for, and mitigate against a terrorist attack. A list of general protective measures for states, localities, the public, and the private sector may not, however, be as effective as state and locally devised protective measures.

---

<sup>22</sup> David A. Fahrenthold, “This Time Orange Alert Seems Less So,” *The Washington Post*, May 22, 2003, p. B2-3.

## Communication of Terrorist Threats to State and Local Governments, the Public, and the Private Sector

DHS uses a variety of communications systems to provide terrorist threat warnings to states, localities, the public, and the private sector. These systems include, for an example, conference calls, public announcements, CEO COM LINK, and NLETS, but DHS has no single communication system it uses to issue HSAS terrorist warnings.

**Analysis and Options.** On April 30, 2003, Jeffery Horvath, chief of the Dover, Delaware police department told the Senate Governmental Affairs Committee that his department has never received any official notification of a change of HSAS threat condition and has relied on the news media for this information. Michael J. Chitwood, chief of the Portland, Maine police department reiterated this point, and specifically identified the Cable News Network (CNN) as the news medium through which he receives notifications of changes in the HSAS threat level. He added that he received official notification from state authorities eight hours later. Fire chief Edward P. Plaugher of Arlington County, Virginia, also identified CNN as the primary source for notification of changes in the HSAS threat level.<sup>23</sup>

When testifying before the Senate Governmental Affairs Committee, DHS Secretary Ridge said that the process for notifying state, and local agencies and authorities of a change in the HSAS threat condition needs improvement.<sup>24</sup>

The public is alerted to a change in HSAS threat condition through the news media, following a public announcement from DHS or media leak of the information. There is no Emergency Alert System (EAS) type communication activated to alert the public to a change in threat condition, so the public is not informed of the change until they monitor a public news source.<sup>25</sup>

Private sector alerts are through CEO COM LINK and conference calls. DHS uses CEO COM LINK to notify private sector entities that participate in the system, and then makes calls to other critical infrastructure and business associations. This arguably results in a de facto prioritization of alerted private sector entities, which could result in a targeted private sector entity being attacked without a timely and effective alert.

**Option 1: Status quo.** Congress may decide to allow DHS to deal with issues relating to HSAS advisories at this stage of HSAS development. This approach would encourage the continued utilization of the DHS terrorist threat communication

<sup>23</sup> U.S. Congress, Senate Governmental Affairs Committee, *Homeland Security and First Responders*, 108<sup>th</sup> Cong., 1<sup>st</sup> sess., April 30, 2003.

<sup>24</sup> U.S. Congress, Senate Governmental Affairs Committee, *State and Local Homeland Security Challenges*, May 1, 2003.

<sup>25</sup> For information on the EAS see CRS Long Report RS21440, "Emergency Communications: The Emergency Alert System and All-Hazard Warnings," by Linda K. Moore, May 15, 2003.

systems. Since the HSAS is designed for federal government use, there may be no need for DHS to establish any other communication systems that disseminate changes in the HSAS terrorist threat levels. This would, however, not address the issues some have raised about the dissemination of HSAS advisories. Some would argue that before DHS establishes a specific system that communicates a change in HSAS terrorist threat levels, DHS needs to establish protective measures for states, localities, the public, and the private sector. This argument is based on the belief that there is little value in knowing of a change in the HSAS terrorist threat level in the absence of recommended protective measures.

*Option 2: Revise the HSAS notification process.* Congress could encourage, or enact legislation instructing, DHS to revise the HSAS notification process to ensure that state and local law enforcement, and emergency management agencies are informed of changes of the terrorist threat level in a more effective and timely manner. This approach could address the problem of states and localities receiving the notification via the news media without first receiving official notification from DHS. This approach, however, would not address the issue of the public, and private sectors receiving timely notification of changes in the HSAS threat level.

## Coordination of HSAS with Other Warning Systems

HSAS is not the only federal warning system: eight separate systems exist to provide timely notification about imminent and potentially catastrophic threats to health and safety.<sup>26</sup> The types of hazards covered by these systems include severe weather,<sup>27</sup> contamination from chemical and biological weapon stockpiles scheduled for destruction,<sup>28</sup> terrorist attacks,<sup>29</sup> and any other emergency or hazard the President decides is significant enough to warrant public notification.<sup>30</sup>

***Analysis and Options.*** Some argue for the consolidation of the existing warning systems into one “all-hazard” system. The Partnership for Public Warning is one organization advocating this type of consolidation.<sup>31</sup> Other organizations, such as the Federal Communications Commission’s (FCC) Media Security and Reliability Council (MSRC) have recommended that the Emergency Alert System (EAS) should

---

<sup>26</sup> For a summary of these warning systems see CRS Report RS21377, *Federal Emergency Warning Systems: An Overview*, by Shawn Reese.

<sup>27</sup> Advanced Weather Information Processing System (AWIPS), Emergency Managers Weather Information Network (EMWIN), National Oceanic and Atmospheric Administration (NOAA) Weather Radio (NWR), and NOAA Weather Wire Service (NWWS)

<sup>28</sup> Federal Emergency Managers Information System (FEMIS)

<sup>29</sup> Homeland Security Advisory System (HSAS)

<sup>30</sup> Emergency Alert System (EAS), and National Warning System (NAWAS)

<sup>31</sup> [<http://www.partnershipforpublicwarning.org>], visited June 10, 2003.

be established and implemented uniformly in all parts of the United States.<sup>32</sup> This enhanced EAS would be fed information from systems such as the HSAS.

Consolidation and coordination of these warning systems would present challenges to administering an “all-hazard” warning system. Some of the challenges include the administration of the warning system, interoperability of existing warning systems, and the involvement of industry.

Congress has directed the President to insure that all appropriate federal agencies are prepared to issue warnings of potential disasters to state and local officials, and that federal agencies provide technical assistance to state and local governments to insure that timely and effective disaster warnings are provided. The President is authorized to utilize or make available to federal, state, and local agencies the facilities of the civil defense communications system, or any other federal communications system, for the purpose of providing warnings to governmental authorities and the civilian population in areas endangered by disasters.<sup>33</sup> Federal agencies that currently administer warning systems include National Oceanic and Atmospheric Administration, Federal Communications Commission, Federal Emergency Management Agency, and Department of Defense. DHS is also responsible for coordinating and distributing warnings to the public.<sup>34</sup>

Existing warning systems are not interoperable. Some of the reasons that warning systems are not interoperable is that the present systems have

- separate transmitting and receiving equipment;<sup>35</sup>
- separate standard message protocols;
- separate procedures for how warnings are input into dissemination systems; and
- separate training, exercising, and testing of the system.<sup>36</sup>

Since this technology is primarily researched, developed, and operated by private industry, the federal government could establish a relationship with the corporate suppliers of these technologies, a relationship to encourage development

---

<sup>32</sup> Molly M. Peterson, “Experts Call For Uniformity in Anti-Terrorism Alert,” *National Journal’s Technology Daily*, May 28, 2003.

<sup>33</sup> 42 U.S.C. 5132.

<sup>34</sup> P.L. 107-296, sec. 102, (c), (3).

<sup>35</sup> This transmitting and receiving equipment include satellite antenna receivers, NOAA Weather Radio, AM and FM radio, television, 1610mHz radio receiver, dedicated computer networks, and dedicated telephone networks.

<sup>36</sup> National Science and Technology Council, Committee on Environment and Natural Resources, *Effective Disaster Warnings*, (Washington: November 2000), pp. 19-20. [http://www.nnic.noaa.gov/CENR/NDIS\_rev\_Oct27.pdf], visited Dec. 23, 2002.

and effectively consolidate or provide the means to make the current warning systems interoperable.

Consolidating and coordinating federal warning systems, however, may cause a loss of concentration on the systems' traditional hazards. Mature warning systems have established alerting protocols and routines that, if consolidated, could become too broad, which may result in less effective warnings.

*Option 1: Status quo.* Without congressional intervention, federal agencies responsible for issuing warnings will likely continue to narrowly focus on traditional hazards. This approach allows mature warning systems to continue communicating alerts and protective measures to an identified audience. Also, this approach would not incur an increased need for federal funding that would be required to update, test, and ensure compatibility of the systems. On the other hand, this approach would not address issues such as overlap of hazards (terrorist threat warnings of HSAS, and any presidential declared emergency warning issued by EAS), and the potential need to reach a wide audience through the use of multiple warning systems.

*Option 2: Coordination and update of warning systems.* If Congress decided to address the issue of coordinating warning systems, it could require all federal agencies with hazard warning responsibilities, to establish, and develop a means for coordinating and updating existing warning systems. This approach could allow any warning of man-made or natural hazards to be issued on the full range of federal warning systems. This could ensure that a larger number of the state and local governments, the public, and private sector entities would receive the specific warning in an effective and timely manner. It would require a communication protocol to be developed that allowed one federal warning system to “talk” to a different system.

Updating of warning systems would not only include the ability of one system to “talk” to another, but could also include the ability of such systems as EAS to be transmitted on off-the-shelf telecommunication devices such as cellular phones. Given the widespread use of wireless communications, some observers have argued for warnings to be issued on wireless devices.<sup>37</sup> In the 108<sup>th</sup> Congress, S. 564 proposes such an approach that would facilitate the deployment of wireless networks in order to extend the range and reach of EAS. It would also ensure emergency personnel priority access to communications facilities in times of emergency.<sup>38</sup>

*Option 3: Consolidation of warning systems.* If Congress decided that there needs to be an all-hazard warning system, it could enact legislation requiring the federal agencies that have warning responsibilities to develop and implement such a system to warn states, localities, the public, and the private sector. This approach could ensure that any warning of a hazard—man-made or natural—would be disseminated to as many entities as necessary in a timely and effective manner. In the 108<sup>th</sup> Congress, two bills, S. 118, and H.R. 2537, propose such an approach to all-hazard warnings. The bills propose the establishment of a single all-hazard warning

---

<sup>37</sup> See footnote 33 on the Partnership for Public Warning.

<sup>38</sup> S. 564, sec. 2, (108<sup>th</sup> Cong.)

system that would ensure that states, localities, the public, and the private sector would be alerted to specific risks from man-made, and natural hazards.<sup>39</sup> This approach, however, would arguably require federal funding and effort to research, test, develop, and implement an all-hazard warning system.

## Cost of Threat Level Changes

An increase in the HSAS threat level imposes both direct and indirect costs on federal, state, and local governments, the private sector, and the public. These costs include the increased security measures undertaken by states and localities, loss to tourism, and the indirect cost on the economy during a period of heightened threat level. Currently, the only cost to states and localities that DHS offers funding for is certain overtime pay due to an increase in the HSAS threat level. In the ODP Critical Infrastructure Protection grant program, state and local first responder agencies may apply and receive funding that assists in paying overtime costs. Also, ODP High Urban Threat Area grant program allows the use of funds to assist in overtime costs.

**Analysis and Options.** Local governments incur direct costs when they put in place additional security measures to deal with a higher threat condition.<sup>40</sup> An example of this is the cost of random car searches at Atlanta's Hartsfield airport, which reportedly requires \$180,000 a month for labor and signage. This cost is borne by Atlanta's police department and airport administration.<sup>41</sup> Because of the budget crisis that many states are experiencing, additional homeland security costs during heightened threat periods are seen as an additional fiscal burden. The costs associated with threat level changes have prompted many state and local officials to complain to DHS.<sup>42</sup> The United States Conference of Mayors released a 145-city survey that reported that during periods of heightened alert homeland security cost increased to additional \$70 million a week.<sup>43</sup>

This increase in homeland security costs during heightened threat periods also has localities arguing for direct funding from the federal government. FEMA's Assistance to Firefighters program and ODP's High Urban Threat Area and Critical Infrastructure Protection grant programs are the only assistance that provide 100% of the funding to localities. ODP's High Urban Threat Area and Critical

---

<sup>39</sup> S. 118, sec. 3, (108<sup>th</sup> Cong.), H.R.2537, sec. 3, (108<sup>th</sup> Cong.)

<sup>40</sup> John Mintz, "U.S. Lowers Level of Terror Alert from Orange to Yellow; Intelligence Suggests Less Risk of Attack," *The Washington Post*, June 1, 2003, p. A4.

<sup>41</sup> Eunice Moscoso, "U.S. Lowers Alert to Yellow But Urges Caution," *The Atlanta Journal-Constitution*, April 17, 2003, p. A3.

<sup>42</sup> John Mintz, and Susan Schmidt, "Government Raises Terror Alert Level to Orange; Officials Say Intelligence Suggests Al Qaeda Attacks," *The Washington Post*, May 21, 2003, sec. p. A1.

<sup>43</sup> Andy Soloman, The United States Conference of Mayors, "War, Threat Alert Increase City Security Costs by \$70 Million per Week Nationwide," press release, March, 27, 2003. Available at: [\[http://www.usmayors.org/uscm/news/press\\_releases/documents/surveyrelease\\_032703.pdf\]](http://www.usmayors.org/uscm/news/press_releases/documents/surveyrelease_032703.pdf), visited Aug. 4, 2003.



Infrastructure Protection grant programs, however, first pass through the state, which causes some localities to complain about a delay in receiving funding.

Authorized program expenditures are another point of contention that states and localities have with homeland security funding and costs. All homeland security grant programs list authorized equipment and activities that grant allocations can be used to fund. States and localities may argue that these authorized expenditures do not address their specific homeland security needs.

These direct homeland security costs occur not only at the state and local level: when the threat level changes, federal departments and agencies have to adopt prescribed protective measures outlined in the different threat condition levels of the HSAS.

An indirect cost of a heightened threat level is the negative effect on tourism in cities perceived as potential targets of terrorism. It has been observed that increased threat levels and the need for heightened security have hurt the tourism industry of such metropolitan areas as Washington, DC, New York, and Chicago. Washington's Mayor Anthony Williams urged residents to be alert for suspicious activities. He also wanted the city to remain friendly, open, and safe to minimize the affects of the terrorist threat level on tourism.<sup>44</sup> D.C. Delegate Eleanor Holmes Norton agreed with the need to keep Washington open to tourism. She said that the city's tourism industry had been hurt by changes in threat condition, and that she feared some officials would overreact and shut down public buildings.<sup>45</sup> An example of the impact on tourism is the decision by some schools to cancel trips to Washington because of the threat of terrorist attack.<sup>46</sup>

Some municipal officials have had to make a costly decision between homeland security and tourism. Philadelphia's mayor, John F. Street, for instance, chose not to close down a street around Independence Hall after he received a call from DHS Secretary Ridge, who advised its closing. Mayor Street cited traffic and tourism concerns as the reason he chose not to respond to the recommendation.<sup>47</sup> Another indirect cost may be how a change in the HSAS threat condition affects the stock markets.<sup>48</sup>

---

<sup>44</sup> Spencer S. Hsu, "Tightening the Security Net," *The Washington Post*, March 19, 2003, p. A1.

<sup>45</sup> Vaishli Honawar, "Tours of Capitol Get Go-Ahead to Resume," *The Washington Times*, April 24, 2003, p. B1.

<sup>46</sup> "New Hampshire News Notes," *The Union Leader*, (Manchester, New Hampshire) March 21, 2003, p. B2.

<sup>47</sup> Alex Fryer, "Feds Guide, Can't Enforce Tight Security at Local Level," *Seattle Times*, May 24, 2003, sec. Domestic News.

<sup>48</sup> Steve Gelsi, "Dow Hits New 2003 High as Stocks Rally," *CBS Market Watch*, May 30, 2003, sec. Market Snapshot. "Stock Market Ticker," *Comtex News Network*, [http://www.briefing.com], May 30, 2003. Eric Kirzner, "War Footing Keeps Markets In Retreat," *National Post's Financial Post & FP Investing*, March 3, 2003, p. FP 7.

*Option 1: Status quo.* Congress may decide that the ODP grant programs adequately meet the needs of states and localities' homeland security costs due to a heightened HSAS threat. It may be an appropriate approach for ensuring the splitting of homeland security costs among the several tiers of government. This policy approach would not however, address such issues as the needs of some state and local first responder agencies, of hiring additional personnel, the loss of revenue generated by tourism due to an increased terrorist threat level, or the cost the economy incurs when the terrorist threat level is raised.

*Option 2: Funding through established ODP grant programs.* Should Congress decide that more funding needs to be provided to cover costs incurred by states and localities due to an increased terrorist threat level, it could consider establishing grant programs that specifically fund such terrorist prevention, preparedness, and mitigation activities as overtime pay for first responders and the purchase of equipment and personnel for the protection of critical infrastructure. In the 108<sup>th</sup> Congress, S. 1245 proposes such an approach by recommending that ODP State Homeland Security Grant program provide up to 5% of appropriated funds for covering the expense of first responder overtime. It also proposes the grant funds be allowed to purchase first responder equipment.<sup>49</sup>

*Option 3: Funding specifically for heightened threat levels.* Should Congress decide to provide funding for costs incurred during heightened threat level periods, it could appropriate funds, in addition to ODP homeland security grant programs, specifically to states, localities, and private sector entities to compensate for costs associated with a change in the HSAS threat level. In the 108<sup>th</sup> Congress, S. 728 proposes such an approach by compensating state and local law enforcement for costs associated with airport security.<sup>50</sup>

---

<sup>49</sup> S.1245, sec. 4, (108<sup>th</sup> Cong.)

<sup>50</sup> S. 728, sec. 4, (108<sup>th</sup> Cong.)